Accelerating the Factorization of Multilinear Boolean Polynomials

Tian Chen and Michael Monagan
tca71@sfu.ca, mmonagan@sfu.ca
Department of Mathematics, Simon Fraser University, Canada

Abstract

A multilinear Boolean polynomial f is a polynomial over GF(2) in which each variable has degree at most 1. Such polynomials arise in Boolean circuit optimization, yet their efficient factorization remains challenging. We present two Monte-Carlo algorithms that advance this problem.

Our first factorization algorithm assumes f is given in the sparse representation. It has algebraic complexity $O(n^2t)$ over a suitable extension field GF(2^k), where n is the number of variables and t is the number of terms of f. Our C implementation achieves substantial speedups over both the FD and GCD algorithms of Emelyanov–Ponomaryov [3]. In our implementation, the dominant bottleneck is multiplication in $GF(2^{63})$; we address this using a compact 64-bit representation together with an optimized bit-shift/XOR reduction routine.

Our second algorithm assumes f is given by a black box $\mathbf{B}$ for its evaluation. Here we apply our recently developed black box factorization algorithm CMBBSHL [1, 2] which is implemented in Maple and C. The black box representation allows us to reduce t (the number of terms of the input polynomial f) to $T = s_{\max}\,(\sum \#f_i + \mathfrak{C}(\text{probe } \mathbf{B}))$ (which can be $\ll t$), where the f_i are the irreducible factors of f, $s_{\max}$ is the maximum number of terms in any coefficient (in the highest ranking variable) in any factor, $\sum \#f_i$ is the total number of terms in all irreducible factors, and $\mathfrak{C}(\text{probe } \mathbf{B})$ is the cost of a single black box probe. This yields an overall algebraic complexity $O(n^2T)$. Our Maple and C implementation of our second algorithm is the fastest algorithm when $T \ll t$.

References

[1] T. Chen and M. Monagan. A new black box factorization algorithm – the non-monic case. In Proceedings of ISSAC 2023. ACM, 2023

[2] T. Chen. Sparse Hensel lifting algorithms for multivariate polynomial factorization. PhD Thesis (2024)

[3] Pavel Emelyanov and Denis Ponomaryov. On a Polytime Factorization Algorithm for Mul- tilinear Polynomials over $\mathbb{F}_2$. Proceedings of CASC 2018, LLNCS 11077:164-176, Springer, 2018.

[4] Jiaxiong Hu and Michael Monagan. A Fast Parallel Sparse Polynomial GCD Algorithm. J. Symb. Cmpt. 105:(1) 28-63, Springer, July 2021.

[5] Amir Shpilka and Ilya Volkovich. On the relation between polynomial identity testing and finding variable disjoint factors. Proceedings of ICALP 2010. LNCS 6198:408-419, Springer, 2010.

[6] Richard Zippel. Probabilistic algorithms for sparse polynomials. Proceedings of EUROSAM '79, LNCS 72:216-226, Springer, 1979.